Réflexions introductives à propos du binôme "Droit-Sécurité"

Poullet, Yves

Published in:
La sécurité informatique entre technique et droit

Publication date:
1998

Document Version
le PDF de l'éditeur

A. RÉFLEXIONS INTRODUCTIVES À PROPOS DU BINÔME "DROIT-SÉCURITÉ"

Yves Poullet

1. DU DROIT À LA SÉCURITÉ

1. "Droit de la sécurité et sécurité des droits" : entre droit et sécurité, le dialogue[1] est enrichissant pour les deux parties car si le droit invite à un renforcement de la sécurité des systèmes d'information, à l'inverse, la sécurisation technique apparaît de plus en plus comme la garantie efficace de la protection des droits.

Deux exemples attesteront de cette interpellation réciproque :

- le souci de la protection des libertés, en particulier de la vie privée a conduit, dès 1981, le Conseil de l'Europe[2] à affirmer le principe de la sécurité des données[3].

Ainsi, en la matière, le droit bouscule la technique et en infléchit le développement. Les débats récents sur l'identification de l'appelant dans les réseaux numériques à intégration de services[4] et sur la structure des

---

1 Cfr. dans le même sens, K. W. K. Kaspersen, Recht en Informatie Technologie : een zaak van intensief onderhoud, Kluwer, 1996, 37 pages.

2 Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel du 28 janvier 1981.

3 L'article 5 de la Convention du Conseil de l'Europe qui affirme la nécessité pour le responsable d'un traitement de prendre les mesures de sécurité appropriées a été largement développé par les articles 16 et 17 de la directive 95/46/CE du Parlement européen et du Conseil de l'Europe du 24 août 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Nous reviendrons amplement sur ce point dans le chapitre consacré aux questions de sécurité et de protection des données (infra, p.).

4 A ce propos, notamment la délibération n° 88-33 du 22 mars 1988 portant avis sur la demande présentée par la Direction générale des télécommunications relative au traitement automatisé de l'identification de la ligne téléphonique appelante entre abonnés au RNIS ouvert commercialement par le département des Côtes du Nord (exp. RNIS/RCNAN), publié comme annexe 36 du 9° rapport d'activité de la

cartes médicales à mémoire délivrées aux patients[5] témoignent parmi bien d'autres de cette contrainte imposée par le droit. A l'inverse, les systèmes de cryptage des messages lors de leur circulation dans les réseaux[6] et plus récemment, les techniques d'anonymisation mises en place par des opérateurs ou serveurs, qui interdisent à l'offreur d'un service télématique de connaître l'identité de celui qui l'interroge, mettent en évidence les bénéfices énormes que peut apporter l'implantation de systèmes techniques dans une protection efficace des droits des personnes concernées. Les commissaires à la protection des données le reconnaissent volontiers[7].

- quittant le domaine du droit à la vie privée, celui des droits d'auteur et droits voisins fournit un exemple de la manière dont la technique peut assurer une protection sans commune mesure avec celle offerte par le droit d'auteur à des œuvres protégées ou non par ce droit. Les "Electronic Copyright Management Systems (E. C. M. S.)" offrent à celui qui y dépose son œuvre dans une banque de données ainsi générées des possibilités de définition et de contrôle automatiques des droits de ceux qui désirent utiliser son œuvre.

CNIL, La Documentation française, 1988, p. 297 ; " L'administration offre aux abonnés concernés la possibilité de refuser au moment de la prise d'abonnement et à titre gratuit qu'à chaque appel émanant de sa ligne son numéro soit communiqué ".

5 A propos des cartes dites " santé ", lire Nguyen NT, Fourez G., Dieng D ;, La santé informatisée, cartes santé et questions éthiques, De Boeck Université, Bruxelles, 1995 ; Poullet, Y., A propos de la propriété du dossier médical, Colloque Faculté de Droit, UFSIA, Namur, De Keure, 1997.

6 La Commission s'est prononcée récemment en faveur de l'utilisation des techniques de cryptographie, considérées traditionnellement comme dangereuses pour la sécurité de l'Etat (Green Paper, Legal Protection of encrypted messages in the internal Market, COM (96) 76 final, 6 mars 1996). Cf. également les lignes directives adoptées par l'OCDE en matière de politiques de cryptographie à sa 31' session des 27 et 28 février 1997 : "Recognizing that as cryptography can be an effective tool for the secure use of I. T. by ensuring confidentiality, integrity and availalibity of data and by providing authentication and non repudiation mechanisms for that data, it is an important component of secure information and communications networks and systems".

7 La Commission (cfr. en particulier l'ouvrage rédigé en commun par les Commissaires de l'Ontario et des Pays-Bas, *Privacy Enhancing Technologies. The path to Anonymity*, vol. I et II, Aug. 95).

- enfin, en droit de la preuve, si les exigences du Code civil requièrent des qualités particulières pour que soient reconnus comme recevables et dotés de force obligatoire les “signatures” et documents électroniques[8].

2. La sécurité apparaît comme un thème majeur des politiques dites d’autoroutes de l’information, tant sa signification est essentielle pour le développement du commerce électronique (cf. les questions de preuve), la protection des investissements mis sur le réseau (cf. les questions de propriété intellectuelle) et la garantie de survie de nos libertés (cf. les questions de protection des données). On conçoit dès lors la place centrale donnée à ce thème par les auteurs de la National Information Infrastructure Policy[9] ou du rapport Bangemann.

La récente communication de la Commission “A European Initiative in Electronic Commerce”[10] retient la sécurité comme premier objectif nécessaire au développement du commerce électronique : “The first objective is to build trust and confidence. For electronic commerce to develop, both consumers and business must be confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to electronic commerce. Yet many remain concerned about the identity and solvency of suppliers, their actual physical location, the integrity of information, the protection of privacy and personal data, the enforcement of contracts at a distance, the reliability of payments, the recourse for errors or fraud, the possible abuses of dominant position considerations which are heightened in cross-border trading”.

3. La perspective du développement des autoroutes de l’information donne à la question de la sécurité une dimension totalement nouvelle : il ne s’agit plus d’assurer la protection des sites, en ce compris contre la poussière, les variations de température et d’humidité, principale préoccupation des

---

8 Sur ces techniques de stations à péage, lire Strowel et J.-P. Triaille, Le droit d’auteur du logiciel au multimédia, Cahier du CRID n° 11, Kluwer, 1996, p. 200 et les nombreuses références y reprises, B. Hugenholtz, Het auteursrecht, het Internet en de informatiesnelweg, N. J. B. , 1995, p. 518.

9 Al Gore, Les “ super autoroutes de l’information ” vont révolutionner le marché de la communication, Discours prononcé devant le National Press Club, Washington, 21 décembre 1993, La revue des discours, n° 7, 1er février 1994.

10 Communication de la Commission au Parlement Européen au Conseil, au Comité économique et Social et au Comité des régions, COM(97) 157, “ disponible sur Internet ”, http : //www.ispo.cec.be/Ecommerce.

années 70 mais de protéger les flux à l'intérieur de systèmes d'information dont l'étendue peut être planétaire. Les applications informatiques autrefois réduites à quelques fonctions générées par un seul ordinateur central volumineux et travaillant en nomade, se sont étendues à des systèmes d'information répartie, systèmes fondés sur une utilisation en réseaux d'une information toujours plus volumineuse et dont les coûts de stockage et de traitement sont en rapport inverse avec la capacité et les potentialités des outils matériels et logiciels.

Cette explosion de la notion de système d'information, d'un site bien identifié à des multiples sites tous en dialogue et aux mains non plus de spécialistes mais de profanes, entraîne l'existence de nombreux risques nouveaux difficiles à circonscrire. L'accès non autorisé ne s'entend plus du franchissement physique d'un sas de sécurité mais bien de la possibilité pour une personne même située à l'autre bout du monde de s'emparer d'un mot de passe ou de pénétrer dans une base de données. L'erreur décelée ne peut être imputée au mauvais fonctionnement de quelques logiciels facilement repérables mais nécessite que soient vérifiés les milliers de maillons qui composent la chaîne reliant l'émetteur et le récepteur d'un message. Le risque a changé de nature et de dimension.

2. DE LA SÉCURITÉ AU DROIT : L'ÉMERGENCE D'UNE "OBLIGATION DE SÉCURITÉ" À TRAVERS LES PRINCIPES DIRECTEURS DE L'OCDE[11].

La sécurité des systèmes d'information a pour objectif de protéger contre les préjudices imputables à des défauts de disponibilité, de confidentialité et d'intégrité, les intérêts de ceux qui, directement (les utilisateurs) ou indirectement (les personnes concernées par les messages soit en tant que sujets, soit en tant que destinataires de ces messages), comptent sur les systèmes d'information.

Une telle définition suppose bien comprise la notion de système d'information, de même que chacune de ces qualités.

---

11 A noter dans le même sens la défunte proposition de décision en matière de sécurité des systèmes d'information, émise par la Commission à l'attention du Conseil (COM(90)314 final - Bruxelles 13 sept. 1990-SYN 288). Cette proposition contenait un plan d'action "to develop a global strategy providing the uses of electronically stored, processed or transmitted information with protection of information systems against and deliberate threats".

A propos de système d'information, les lignes directrices de l'O.C.D.E. régissant la sécurité des systèmes d'information édictées en décembre 1992[12], distinguent les notions de données, d'information et de systèmes d'information :

"- par "données", on entend une représentation de faits, de concepts ou d'instructions sous une forme adaptée à la communication, à l'interprétation ou au traitement par des êtres humains ou des machines;"

"- par "informations", on entend la signification que prennent les données du fait des conventions qui s'attachent à ces données[13];"

"- par "systèmes d'information", on entend les ordinateurs, installations de communication et réseaux d'ordinateur et de communication ainsi que les données et informations qu'ils permettent de conserver, de traiter, d'extraire ou de transmettre y compris les programmes, spécifications et procédures destinés à leur fonctionnement, utilisation et maintenance."

La sécurité d'un système d'information consiste à en préserver la disponibilité, la confidentialité et l'intégrité. Les lignes directrices de l'O.C.D.E. déjà citées définissent comme suit ces diverses qualités : " la disponibilité[14] est, pour des systèmes d'information, le fait d'être accessibles et utilisables en temps voulu et de la manière requise; la confidentialité est pour des données et des informations, le fait d'être uniquement portées à la connaissance des personnes, entités ou mécanismes autorisés, à des moments autorisés et d'une manière autorisée; l'intégrité est, pour des données ou des informations, le fait d'être exactes et complètes et de préserver ce caractère exact et complet".

Quelques principes tendant à assurer le respect de cette obligation de sécurité sont énoncés par les lignes directrices de l'O.C.D.E.. Quelques

---

12 publié par l'OCDE, G. D. (92)190, Paris, déc. 1992.

13 la distinction entre "donnée" et "information" est classique dans la doctrine française. A ce propos, entre autres, les travaux de A. Bertrand, 1991, p. 438 et s. et les nombreuses références notamment aux travaux de Catala.

14 Certains distinguent de la disponibilité, la continuité du système d'information, c'est-à-dire le fait de maintenir le système à tout moment de sa vie conforme aux nécessités de l'utilisateur. Ceci implique non seulement les activités de prévention et d'intervention en cas d'incidents, mais également les activités d'adaptation du système à des besoins nouveaux, ainsi en cas de modification d'une législation ou d'un élément de l'environnement technique.

commentaires à leur propos sont, nous semble-t-il, utiles[15]. - le principe de responsabilité exige la claire répartition des responsabilités entre les différents intervenants à la conception, à la réalisation et à l'exploitation d'un système d'information, qu'il s'agisse des fournisseurs, des gestionnaires, des propriétaires et bien évidemment des utilisateurs tant internes qu'externes. Ce partage des responsabilités doit être l'objet de clauses contractuelles précises[16] ou de dispositions réglementaires adéquates.

- le principe de sensibilisation insiste sur la nécessaire information des différentes parties intervenantes à propos de l'existence et des modalités des mesures de sécurité. Cette sensibilisation est considérée comme nécessaire pour instaurer la confiance de tous. Une telle réflexion est particulièrement pertinente en ce qui concerne les employés d'une entreprise. L'utilisation des technologies de l'information autorise nombre de traitements conduisant à une surveillance ou un contrôle de leurs activités et ce, à des fins de sécurité *a priori* légitimes. Les dispositions des législations de protection des données instaure au profit des personnes concernées un droit à l'information sur l'existence, les finalités des traitements et la nature des données y traitées, en même temps qu'il ouvre à ces personnes un droit d'accès[17]. Le respect de ces divers droits conduit à justifier l'information individuelle non seulement des travailleurs mais également collective[18].

- le principe d'éthique consacre la nécessité d'une prise en considération lors de l'implantation de systèmes de sécurité de l'intérêt légitime des tiers. Par tiers, on songe tant aux personnes concernées par l'information traitée ou véhiculée qu'aux concurrents. Ainsi à propos de ces derniers, on conçoit aisément que pour des motifs soi-disant de sécurité, l'utilisation d'un système d'information pourtant stratégique à l'intérieur d'un secteur soit réservée à quelques entreprises et fermée à d'autres. L'exemple des services aériens développés au départ par des groupes de transporteurs bien fermés montre que le principe éthique a trouvé dans le droit de la

---

15 Le lecteur trouvera en annexe de la présente contribution, le texte de ces principes.

16 A cet égard, nous renvoyons le lecteur à la contribution de B. Lejeune, Aspects contractuels de la sécurité informatique, *infra*, p ...

17 ll s'agit des articles 10 et 11 de la directive européenne en matière de protection des données déjà citéee.

18 Cf. à ce propos, la recommandation adoptée par les commissaires de la protection des données lors de leur réunion d'Ottawa le 19 septembre 1996 : Privacy in Labour relationships.

concurrence un précieux relais obligeant ces services à s'ouvrir à tout transporteur satisfaisant aux conditions y compris de sécurité de l'utilisation du service[19].

- le principe de pluridisciplinarité exige que les questions de sécurité des systèmes d'information soient abordées conjointement par des techniciens certes, mais également des juristes, des spécialistes de la gestion économique et administrative, voire de l'éducation. C'est que l'implantation de systèmes de sécurité représente un coût mais également des avantages qui ne se mesurent pas purement en termes de rentabilité financière, c'est qu'il suppose des choix techniques et impose des modifications aux flux d'information existant à l'intérieur des entreprises mais également à l'extérieur. I1 impose à chaque utilisateur de nouvelles pratiques (p. ex. la gestion de son mot de passe) qui impliquent une formation idoine.

- le principe de proportionnalité n'est autre que la consécration de manière générale d'une disposition déjà existante en matière de vie privée : "Les Etats-membres prévoient que le responsable du traitement doit mettre en oeuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre tout autre forme de traitement illicite."

Ces mesures doivent assurer, "compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard de risques présentés par le traitement et de la nature des données à protéger"[20].

Ce même principe de proportionnalité se retrouve, selon certains[21] en droit de la preuve où les exigences en matière de signature et de document

---

19 A ce propos, le règlement du Conseil n°2299/89 (J. O. n° L 220 du 29. 7. 89) instaurant un code de conduite pour l'utilisation de systèmes informatisés de réservation aérienne suivie d'une notice explicative de la Commission (J. O. n° C. 184 du 25. 7. 1990, p. 2).

20 C'est le libellé même de l'article 17 de la directive européenne relative à la protection des données.

21 "L'on s'est accordé à penser que les règles uniformes applicables aux signatures électroniques devraient avoir pour objet de donner aux législateurs des indications sur les techniques de nature à remplir une multitude de fonctions d'authentification dans un milieu électronique. Ces techniques se classaient le long d'une échelle mobile allant du degré de sécurité le plus élevé (…) au degré de sécurité relative offert par les

électronique pourraient varier selon la nature et le montant des transactions en tenant compte notamment de la probabilité et de l'ampleur des éventuels préjudices liés à cette transaction. En droit pénal, le même principe a parfois justifié l'affirmation selon laquelle le bénéfice des poursuites pénales devait être réservé à celui qui a pris les mesures de sécurité nécessaires pour éviter le succès de l'infraction ou de sa tentative[22].

- le principe d'intégration exige une approche et une stratégie globales et non fragmentées[23]. I1 s'agit de ne pas dissocier les aspects techniques de ceux du management. Ainsi, si la sécurité d'un système d'information prévoit la distribution de clés, il est important que cette distribution suive les règles hiérarchiques prévues par ailleurs.

- le principe d'opportunité souligne la nécessité d'actions prises en temps utile, coordonnées entre partenaires publics et privés et décidées tant au niveau national qu'international. Si on songe bien évidemment à la coopération policière en matière de répression de la criminalité informatique, on peut également concevoir des règles communes prises au sein des organes de standardisation et fixant les principes selon lesquels doivent opérer les organes de standardisation[24]. Enfin on citera des

---

marques manuscrites ou les tampons" (Rapport du groupe de travail sur le commerce électronique, déjà cité, n° 21). Cf. même principe dans le Computer Security Act de 1987 (Pub. Law 100. 235) qualifié de Risk Based Standard. Il s'agit de fixer les exigences en matière de preuve et de signatures en fonction des "risk and magnitude of the damages resulting from the loss, misuse or unauthorized access or modification of the information".

22 Ainsi, en Allemagne, l'accès non autorisé n'est reprimé que pour autant qu'il y ait eu violation d'une règle de sécurité (art. 203 du code pénal allemand).

23 Comp. : "An overall strategy considering all aspects of security of information systems, needs to be established, avoiding a fragmented approach" (Summary of action lines, Orientations for an action plan in the field of the security of information systems, J. O. C. E. , 8. 5. 92, n° L 123/22).

24 Cf. à cet égard, les réflexions de C. Stuurman, Legal Aspects of Standardization and certification of Information Technology and Telecommunications : an Overview, Data Security in Computer Networks and Legal problems, W. Kilian and A. Wiebe (ed.), Beitrage zür juristischen Informatik, T. 17, S. Toechl Mittler Verlag, 1992, p. 95 et s.

initiatives comme celle d'Eurocards[25] réunissant des organismes privés subsidiés par la Commission européenne et chargés de définir les conditions tant techniques, juridiques et éthiques du développement de cartes santé.

- le principe de réévaluation traduit la nécessité de révision périodique des exigences de sécurité. A titre d'exemple, on citera la question de la longueur des clés de chiffrement acceptables pour faire preuve d'une transaction électronique. Les possibilités de déchiffrement des moyens modernes obligent à ne plus se contenter de clés de 50 ou 60 caractères mais bien de 80 caractères voire plus afin de garantir une robustesse suffisante.

- le principe de démocratie conclut la liste des principes de l'O.C.D.E. Il convient que "la sécurité des systèmes d'information soit compatible avec l'utilisation et la circulation légitime des données et informations dans une société démocratique". Un tel énoncé du principe est peut-être réducteur dans la mesure où il ne souligne pas la nécessité de suivre, en la matière, des procédures de décision qui permettent à chaque groupement d'intérêt de s'exprimer. Ainsi, nous l'avons déjà signalé[26], dans l'entreprise, les

---

25 Sur les aspects juridiques et éthiques de ce programme Eurocards, lire P-A. Comeau et Y. Poullet (éd.), The Health card and its users/ Sociological Questions and Legal issues, Eurocards Concerted Action, AIM/DGXIII, E.C., Aug. 1996.

26 A cet égard, la convention collective de travail du 19 mai 1995 signée au sein de la Commission paritaire pour les sociétés de prêt hypothécaire, d'épargne et de capitalisation et relative à l'information et la concertation sur les conséquences sociales de l'introduction de nouvelles technologies rendue obligatoire par l'A. R. du 7 août 1996 (M. B. , 27 nov. 1996, p. 29833). "Art. 3. Les parties reconnaissent que l'introduction ou l'adaptation de procédés de travail technologique :

- est indispensable pour le développement économique et pour le maintien de la position concurrentielle des banques d'épargne;

- relève de la responsabilité de gestion exclusive du chef d'entreprise;

- doit être située, non seulement dans le cadre de l'utilité technique et économique - ou de la nécessité technique et économique - pour l'entreprise mais aussi dans le cadre des conséquences que l'introduction peut avoir au niveau social, plus particulièrement en ce qui concerne l'emploi, l'organisation du travail et les conditions de travail;

- doit donner lieu à une information aux organisations représentatives de travailleurs et à une concertation avec celles-ci au sein de l'entreprise concernée, et ceci dans les cas et selon les modalités prescrites dans la

procédures de contrôle et de surveillance des activités des employés devraient faire l'objet de débats dans les organes de participation (nos conseils d'entreprise). A un niveau national, des décisions comme celle de créer des services de certification électronique devraient être éclairées par un débat préalable où doivent être entendus les représentants des consommateurs et des personnes défavorisées afin d'éviter qu'ils ne soient exclus de l'accès à de tels services.

L'énoncé du principe met en évidence la nécessité d'opérer une balance d'intérêts entre les objectifs de sécurité que légitimement certains peuvent poursuivre et d'autres objectifs comme la non discrimination, la sécurité publique, l'accès de tous à certaines informations. Quelques exemples : les E. C. M. S. dont nous avons parlé, représentent certes un outil extraordinaire de protection des intérêts des auteurs. Ne faut-il cependant pas que, vis-à-vis de certaines informations, l'accès de tous soit garanti à un prix abordable ? La notion de service universel défini comme l'accès de tous à certains services d'intérêt général est également une manière de lutter contre les appropriations exclusives d'informations ou de services que facilite la mise en place de dispositifs de sécurité. On connaît à ce sujet la pratique des licences obligatoires. La cryptographie représente certes un instrument de sécurisation des messages mais son développement anarchique peut mettre en danger les intérêts de la sécurité publique rendant impossible la détection de messages attentatoires à celle ci[27].

L'obligation n'est pas entendue ici dans son sens strict du droit civil comme découlant soit d'un contrat, soit des règles régissant la responsabilité civile. La notion est entendue dans un sens plus large comprenant toutes les exigences nécessaires à assurer la sécurité informatique telle que définie ci-avant et découlant non seulement des

---

convention collective de travail n° 39 du Conseil national du travail du 13 décembre 1983, concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies. En outre, les organisations représentatives des travailleurs seront informées préalablement par le chef d'entreprise, des changements susceptibles de modifier les conditions de travail contractuelles ou habituelles. Toute information doit être fournie dans un langage compréhensible". Sur la nécessité d'un consensus à propos de l'introduction de technologies dites sécurisantes comme la carte santé, lire le rapport d'Eurocards cité supra note 25.

27 Sur les débats à propos de cryptographie, lire les réflexions de M. Antoine, *infra* p. …et les recommandations de l'OCDE en la matière (Guidelines for cryptography policy) en date du 27/3/97, disponible à http : //www.oecd.org/dsto/iccp/crypto.e.html.

dispositions générales du Code Civil, mais aussi des lois et réglementations particulières, voire des codes de bonne conduite professionnelle.

Le titulaire de l'obligation est déterminé par le texte qui est à la source de celle-ci. On soulignera qu'en matière informatique, la multiplicité des parties impliquées dans la mise en place et le fonctionnement d'un système peut compliquer cette détermination. On recommandera dès lors d'user à ce sujet de la liberté contractuelle prévue par l'article l 134 du Code Civil sans toutefois empiéter sur les dispositions d'ordre public ou impératives. Ainsi, en tant que *"professionnel",* le fournisseur d'un système de sécurité ne pourra se dégager de la garantie des vices cachés en la reportant sur une autre partie.

Traditionnellement, le rôle du droit est de trois ordres : prévenir, réparer et sanctionner.

Face aux problèmes posés par la sécurité du système d'information, ce triple rôle du droit peut s'analyser comme suit :

l. Le rôle peut aider à prévenir les risques informatiques c'est-à-dire proposer des solutions contractuelles qui permettent à l'utilisateur de diminuer voire d'évacuer certains risques;

2. En cas de survenance du risque, le droit peut prévoir des solutions de remplacement, solutions financières bien souvent;

3. Enfin, la faute humaine à la base du sinistre mérite parfois d'être sanctionnée.

Le rôle préventif du droit est assuré essentiellement par le droit des contrats. L'intégrité des données, la fiabilité des traitements et la confidentialité des résultats feront l'objet de clauses particulières dans les contrats portant sur la fourniture du hardware, du logiciel mais également dans les contrats d'emploi et dans les contrats *"télématiques"*. Ils peuvent faire l'objet de contrats ou prestations particulières auprès de tiers, chargés de valider les programmes. Le maintien des différentes qualités du logiciel tout au long de la vie du système sera assuré par des clauses particulières du contrat de maintenance.

Le rôle curatif du droit est l'objet de contrats spéciaux : contrats de back-up d'une part, contrat d'assurance d'autre part. Il est également garanti par les multiples clauses de réparation des dommages proposés dans les différents contrats conclus avec les fournisseurs.

Enfin, une lourde sanction pénale est parfois le meilleur moyen pour dissuader les personnes susceptibles d'être les auteurs d'un sinistre. A cet égard, le droit pénal a certes à s'adapter aux nouvelles infractions permises

par les nouvelles technologies de l'information. Dans cet ouvrage, le droit pénal des NTIC ne sera invoqué qu'incidemment[28].

Ce triple rôle, le droit peut le jouer en fonction d'intérêts divers :

- il s'agira tout d'abord de protéger les intérêts d'un utilisateur de système d'information dans l'acquisition des éléments de son système d'information, c'est-à-dire en tant qu'acquéreur d'éléments matériels ou logiciels mais également face aux risques de son fonctionnement;

- il s'agira ensuite de protéger les intérêts des particuliers en assurant, d'une part, la sécurité de l'infrastructure qui permettra la transaction (sécurité du réseau), mais également et surtout, la fiabilité tant de contenu que juridique de leur transaction. Se trouve posée par ce second point, la question de la recevabilité à titre de preuve des enregistrements électroniques;

- il s'agira enfin de protéger les intérêts de tiers auxquels se réfère l'information collectée, stockée ou communiquée : c'est toute la question des législations dites de protection des données ou "Privacy".

---

28 A cet égard, le lecteur se référera à l'article de Ph. Gérard et V. Willems, Prévention et répression de la criminalité sur Internet, in Internet face au droit, E. Montero (éd.) Cahier du CRID n° 13, p. 144 et s. Cf également P. van Eecke, Criminaliteit in Cyberspace, Min. van Justicie, VIII, éd. Mijs-Breesch, 1997.